GOVERNMENT OF INDIA
COMMUNICATIONS AND INFORMATION TECHNOLOGY
LOK SABHA

UNSTARRED QUESTION NO:672
ANSWERED ON:27.04.2016
Cyber Crimes
Hari Shri G.;Kamaraaj Dr. K.;Singh Shri Dushyant

Will the Minister of COMMUNICATIONS AND INFORMATION TECHNOLOGY be pleased to state:

(a) the details of the major and minor Cyber Attacks which have been attempted on the Government websites/databases during the last year;
(b) whether there has been a loss/theft/adulteration of significant data through these attacks;
(c) if so, the details thereof; and
(d) the steps taken by the Government to deal with this grave cyber security issue?

Answer

(a): As per the information reported to and tracked by Indian Computer Emergency Response Team (CERT-In), a total number of 164 Government websites were hacked during the year 2015.

(b) and (c): The Government websites host information for public dissemination. No sensitive information is hosted on Government websites. As per the guidelines of the Government, the Computer systems with sensitive information are isolated from Internet.

(d): Government has taken the following steps to enhance cyber security and to protect the websites:

i. The Indian Computer Emergency Response Team (CERT-In) regularly tracks the hacking of websites and alerts the website owners concerned to take actions to secure the websites to prevent recurrence.
ii. CERT-In issues alerts and advisories regarding latest cyber threats and countermeasures on regular basis. CERT-In has published guidelines for securing the websites, which are available on its website (www.cert-in.org.in). CERT-In also conducts regular training programmes to make the system administrators aware about secure hosting of the websites.
iii. In order to protect the websites of Government departments a layered security approach in the form of practices, procedures and technologies is put in place. National Informatics Centre (NIC) that hosts the Government websites has deployed state-of-the-art security solutions including firewall, intrusion prevention systems and anti-virus solution.
iv. All major websites are being monitored regularly to detect malicious activities. A 24x7 security monitoring centre is operational in NIC for responding to security incidents. The security events generated from various security solutions on NIC Network (NICNET) are monitored round the clock for taking remedial measures.
v. All Central Government Ministries / Departments and State / Union Territory Governments have been advised to conduct security auditing of entire Information Technology infrastructure. All the new government websites and applications are to be audited with respect to cyber security prior to their hosting. The auditing of the websites and applications is to be conducted on a regular basis after hosting also. Indian Computer Emergency Response Team (CERT-In) provides necessary expertise to audit IT infrastructure of critical and other ICT sectors.
vi. Government has formulated Crisis Management Plan for countering cyber attacks and cyber terrorism for implementation by all Ministries/ Departments of Central Government, State Governments and their organizations and critical sectors.
vii. Cyber security mock drills are being conducted regularly to enable assessment of cyber security posture and preparedness of organizations in Government and critical sectors.

****